

United States Courts
Southern District of Texas

FILED

November 21, 2024

Nathan Ochsner, Clerk of Court

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

FILED
U.S. DISTRICT COURT
MIDDLE DISTRICT OF TENN.

NOV 06 2024

DT

DEPUTY CLERK

UNITED STATES OF AMERICA

v.

[1] SAMSON A. OMONIYI

a/k/a "Dada"

a/k/a "Dadaman81"

a/k/a "Mr D"

UNDER SEAL

No. 3:24-00197

4:24-mj-508

I N D I C T M E N T

THE GRAND JURY CHARGES:

At all times relevant and material to this Indictment:

INTRODUCTION

1. [1] **SAMSON A. OMONIYI**, a/k/a “Dada,” a/k/a “Dadaman81,” a/k/a “Mr D,”
was a citizen of Nigeria residing in the Southern District of Texas.

2. [REDACTED]
[REDACTED]
[REDACTED]

3. [REDACTED]
[REDACTED]

4. [REDACTED]
[REDACTED]

5. [REDACTED]
[REDACTED]

6. [REDACTED]
[REDACTED]

7. [REDACTED]
[REDACTED]

8. [REDACTED]
[REDACTED]

9. [REDACTED]
[REDACTED]

BACKGROUND

10. Criminals use the internet to perpetrate fraud schemes against victims in the United States and abroad that involve billions of dollars of losses per year. These frauds can include “business email compromise” schemes (“BEC” schemes). Scammers rely on networks of individuals to launder the fraud proceeds through the U.S. financial system in a manner that, among other things, conceals and disguises the nature, location, source, ownership, and control of those proceeds. Defendants laundered proceeds of internet fraud scams, including BEC schemes.

11. A BEC is a type of fraud scheme that targets victim companies that conduct business routinely through wire transactions. Scammers engage in multiple schemes to infiltrate the emails of a victim company’s employees, who frequently are responsible for conducting wire transfers. The scheme may occur initially when an employee of a victim company is tricked into interacting with a scammer who sent the email message that appears to be, but is not, legitimate. For example, the scammer may have added a single letter to an email address or changed or removed a letter or number from an email address known to the victim such that the victim does not notice the difference. This is commonly referred to as “spoofing.” Perpetrators engaged in BEC schemes may also gain access to a victim company employee’s or client’s email account and learn of pending financial transactions. Scammers use their access to a victim’s email address to target the financial transaction and redirect money related to a financial transaction to accounts held by a scammer’s co-conspirators.

12. Typically, in a BEC scheme, the scammer sends an email to an employee at the victim company who serves a role in the victim company’s finance department or senior leadership. After gaining sufficient intelligence about the victim’s activities, the scammer may send additional fraudulent emails to either the victim company employee who originally received

the fraudulent email, or to someone communicating with the victim company employee, requesting payment to a vendor known to the victim company or for goods and services allegedly purchased by the victim company. Because the scammer is familiar with the victim company's employee's role and any pending financial obligations related to the victim company, the scammer writes emails to convince the recipient that the victim company's request for payment was genuine. The fraudulent emails written by the scammer may take several forms, including emails from fake email accounts that closely resemble legitimate business emails that direct payment to bank accounts held by the scammer's co-conspirators, or emails from legitimate but hacked email accounts directed internally within the victim company or to third parties, sometimes containing false invoices that direct payment to bank accounts held by the scammer's co-conspirators.

13. A money laundering organization ("MLO") is a group of associated individuals who have agreed to launder proceeds of unlawful activity. For example, MLOs may receive fraudulent proceeds generated from illegal activities, such as a BEC.

14. MLOs transfer the fraudulent proceeds in a concealed manner, among other methods, to other members of the MLO and, at times, funnel those proceeds back to those perpetrating the fraud. MLOs may work directly with or on behalf of the scammers to enable them to receive the proceeds generated from their fraud.

15. MLOs frequently use "money mules" to help launder proceeds derived from fraud schemes, such as BEC schemes. A "money mule" is an individual who has been recruited by a "herder" or recruiter to use a bank account belonging to the "money mule" to transfer and conceal proceeds derived from fraud. The "herder" or recruiter instructs a "money mule" to move the proceeds through the U. S. and foreign banking systems by various physical and electronic means,

including but not limited to wire transfers, cashier's checks, peer-to-peer payment platforms, money services businesses, withdrawals of cash, or a combination of these means.

16. MLOs can employ a structured organization, which is compartmentalized to protect its members. For example, a lower-level member in the MLO, like a "money mule," may not know other lower-level members or those in positions senior to them other than their "herder(s)" recruiter(s).

17. A "front company" is a legally established business entity made to appear operational. It is typically used to give the impression that there is a legitimate business involved in the scheme. Although a front company may engage in some legitimate business activities, MLOs primarily use front companies to conceal the nature, source, ownership, and control of proceeds of unlawful activity.

18. A "sham company" does not engage in legitimate business activities and is often used by MLOs to conceal the nature, source, ownership, and control of proceeds of unlawful activity.

BEC FRAUD SCHEME

19. Cooperating Witness 1 ("CW 1"), Cooperating Witness 2 ("CW 2"), D.E., Z.M., D.T., D.V., N.P., S.H., P.S, and D.W., all individuals known to the Grand Jury, are "money mules."

20. COMPANY A is a real estate investment and consulting firm located in Florida.

21. COMPANY B is a construction company located in Idaho.

22. COMPANY C is a financial management company located in California.

23. COMPANY D is a medical services provider located in Alabama.

24. COMPANY E is a software development company located in Texas.

25. COMPANY F is a solar lighting company located in California.

26. COMPANY G is a construction company located in New Jersey.
27. COMPANY H is a global supply chain management business located in France.
28. COMPANY I is a constructions material company located in Canada.
29. COMPANY J is a biotechnology company located in California.
30. COMPANY K is an escrow company located in California.
31. COMPANY L is a solar panel manufacturing company located in Missouri
32. The Defendants' co-conspirators, unknown to the Grand Jury, devised and intended to devise a scheme to defraud the victims, including victim COMPANIES A through L and their employees or clients, to obtain money and property by means of false and fraudulent pretenses, representations, and promises. To achieve these ends, the Defendants' co-conspirators, unknown to the Grand Jury, engaged in the following acts:

- a. On or about November 25, 2016, Defendants' unknown co-conspirators spoofed the employee email account of W.Z., a realtor employed by COMPANY A. The perpetrators of the compromise caused COMPANY A's customer on or about November 25, 2016, to make a \$97,335 payment for the customer's real estate investment to a Regions Bank account ending in x5201, controlled by [REDACTED] and "money mule" D.E., held in the name of sham company West Wego Resources.
- b. On or about August 28, 2017, Defendants' unknown co-conspirators gained unauthorized access to the business email account of B.G., the President of COMPANY B. The perpetrators of the compromise caused COMPANY B's employee, on or about September 11, 2017, to wire \$180,000 from COMPANY B's bank account to the Woodforest Bank account ending in x0279, controlled by

“money mule” R.W., held in the name of R.W.’s business. Additionally, on or about September 12, 2017, the perpetrators of the compromise caused COMPANY B’s employee to wire \$269,800 from COMPANY B’s bank account to a Diversified Members Credit Union bank account ending in x3097, controlled by “money mule” J.B.

- c. On or about October 10, 2017, Defendants’ unknown co-conspirators gained unauthorized access to the email account of R.D., a client of COMPANY C. The perpetrators of this compromise caused COMPANY C’s employee, on or about October 10, 2017, to wire \$9,670 from R.D.’s family member’s bank account to the Ascend Federal Credit Union account ending in x7865, controlled by [REDACTED]

[REDACTED] held in the name of sham company R & MC Productions.

- d. On or about June 7, 2018, Defendants’ unknown co-conspirators spoofed an employee email account at COMPANY D. The perpetrators of this compromise caused COMPANY D’s employee, on or about June 7, 2018, to wire \$23,159 from COMPANY D’s bank account to the Regions Bank account ending in x7495, controlled by [REDACTED], held in the name of sham company End Staff Remodeling. Additionally, on or about June 8, 2018, the perpetrators of this compromise caused an employee of COMPANY D to wire \$25,968 to the same Regions Bank account ending in x7495, controlled by [REDACTED] held in the name of sham company End Staff Remodeling.

- e. On or about July 17, 2018, Defendants’ unknown co-conspirators spoofed the business email account of R.J., the CEO and President of COMPANY E. The perpetrators of this compromise caused COMPANY E employee D.J., on or about

July 17, 2018, to wire \$59,900 from COMPANY E's bank account to the First Tennessee Bank account ending in x0420, controlled by CW 1, held in the name of CW 1's business. Additionally, the perpetrators of this compromise, caused COMPANY E's employee D.J., on or about July 18, 2018, to wire \$89,900 from COMPANY E's bank account to the same First Tennessee Bank account ending in x0420, controlled by CW 1, held in the name of CW 1's business.

- f. On or about September 13, 2018, Defendants' unknown co-conspirators spoofed the business email account of D.S., the president and CEO of COMPANY F. The perpetrators of this compromise caused COMPANY F's employee, A.T., on or about September 13, 2018, to wire \$9,880 from COMPANY F's bank account to the First Tennessee Bank account ending in x3289, controlled by [REDACTED] [REDACTED] held in the name of sham company EDC Tooling.
- g. On or about December 12, 2018, Defendants' unknown co-conspirators gained unauthorized access to the business email account of M.H., an employee of COMPANY G. The perpetrators of this compromise caused COMPANY G's customer, on or about December 14, 2018, to wire \$674,202.56 to the SunTrust Bank account ending in x1305, controlled by "money mule" Z.M., held in the name of Z.M.'s business.
- h. On or about February 3, 2021, Defendants' unknown co-conspirators compromised the business email account of A.M., an accountant at COMPANY H. The perpetrators of this compromise caused COMPANY H's client, on or about March 8, 2021, to wire \$97,627.08 from COMPANY H's client's bank account to the Bank of America account ending in x6217, controlled by "money mules" D.V. and N.P.,

held in the name of D.V. and N.P.'s business. Additionally, the perpetrators of this compromise caused COMPANY H's client, on or about May 14, 2021, to wire \$60,890.31 from COMPANY H's client's bank account to the same Bank of America account ending in x6217, controlled by D.V. and N.P.

- i. On or about April 12, 2021, Defendants' unknown co-conspirators compromised the business email account of P.W., a senior employee at COMPANY I. The perpetrators of this compromise caused COMPANY I's client, on or about April 20, 2021, to wire \$103,978.46 from COMPANY I's client's bank account to the Bank of America account ending in x8356, controlled by "money mule" R.M.
- j. On or about November 2, 2021, Defendants' unknown co-conspirators spoofed the business email account of L.G., an accountant for COMPANY J. The perpetrators of this compromise caused COMPANY J's vendor, on or about November 9, 2021, to wire \$250,000 from COMPANY J's vendor's bank account to the Wells Fargo bank account ending in x4950, controlled by CW 2, held in the name of CW 2's business.
- k. On or about March 9, 2022, Defendants' unknown co-conspirators gained unauthorized access to R.P.'s email account. R.P. was a client of COMPANY K, a financial services company in control of R.P.'s trust funds. The perpetrators of this compromise caused COMPANY K's employee, on or about March 28, 2022, to wire \$319,902.56 - belonging to R.P. - from COMPANY K's bank account to the Wells Fargo bank account ending in x2882, controlled by "money mule" S.H., held in the name of S.H.'s business.

1. On or about June 8, 2022, Defendants' unknown co-conspirators gained unauthorized access to T.C.'s business email account. T.C. was a director at COMPANY L. The perpetrators of this compromise caused COMPANY L's customer, on or about June 23, 2022, to wire \$250,000 from COMPANY L customer's bank account to the Regions Bank account ending in x3093, controlled by "money mule" D.W., held in the name of D.W.'s business.

COUNT ONE

Conspiracy to Commit Money Laundering
(18 U.S.C. § 1956(h))

33. Paragraphs 1 through 32 are re-alleged and incorporated by reference as if fully set forth herein.

34. Beginning on a date unknown to the Grand Jury, but from at least in or about November 2016, and continuing through at least in or about the date of the return of this Indictment, the exact dates being unknown to the Grand Jury, in the Middle District of Tennessee, the Southern District of Texas, and elsewhere, Defendants [1] **SAMSON A. OMONIYI**, a/k/a "Dada," a/k/a "Dadaman81," a/k/a "Mr D"; [REDACTED]

[REDACTED], and others to the Grand Jury known and unknown did knowingly and voluntarily combine, conspire, and agree with one another, and with other persons known and unknown to the Grand Jury, to commit offenses against the United States, to wit:

- a. to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which involved the proceeds of specified

unlawful activity, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, knowing that said transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and knowing that the property involved in said financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and

- b. to knowingly engage and attempt to engage, in monetary transactions by, through, or to a financial institutions, affecting interstate and foreign commerce, in criminally derived property of a value greater than \$10,000, such property having been derived from a specified unlawful activity, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, in violation of Title 18, United States Code, Section 1957.

OBJECT OF THE CONSPIRACY

35. The object of the conspiracy was to enrich members of the conspiracy through the laundering of fraudulent proceeds obtained through fraud scams, including BEC schemes identified above, occurring throughout the United States, including in the Middle District of Tennessee.

MANNER AND MEANS

36. The object of the conspiracy was to be accomplished by the following ways, manner, and means, among others:

- a. It was part of the conspiracy that Defendants, unindicted co-conspirators, and others known and unknown to the Grand Jury took on different roles in the conspiracy,

including participating in the conspiracy through various acts as “money mules,” “herders,” or recruiters.

- b. It was further part of the conspiracy that Defendants, unindicted co-conspirators, and others known and unknown to the Grand Jury laundered fraud proceeds that were derived from frauds, including the BEC schemes identified above, executed against unsuspecting victims located throughout the United States, including an agency of the State of New Jersey, and in foreign countries, including Canada, France, and Bolivia, which caused the victims to transfer monies from bank accounts controlled by the victims to accounts controlled by Defendants and others known and unknown to the Grand Jury.
- c. It was further part of the conspiracy that Defendants, unindicted co-conspirators, and others known and unknown to the Grand Jury laundered the fraudulent proceeds generated from the BEC and other fraud schemes, so those proceeds were received by and distributed among the members of the conspiracy. The Defendants and other co-conspirators attempted to generate and launder over \$20 million in fraud proceeds derived from BEC and other Internet fraud schemes.
- d. It was further part of the conspiracy that Defendants, unindicted co-conspirators, and others known and unknown to the Grand Jury, including CW 1, agreed to and did establish numerous personal and business bank accounts at financial institutions for the purpose of receiving fraudulent proceeds derived from the BEC schemes.
- e. It was further part of the conspiracy that Defendants, unindicted co-conspirators, and others known and unknown to the Grand Jury caused the following sham or

front companies, among others, to be established and used to open bank accounts at financial institutions in the following company names:

| Sham or Front Company | Defendant(s) Associated With |
|---|------------------------------|
| West Wego Resources LLC a/k/a Westwego Resources LLC | [REDACTED] |
| R & MC Productions | [REDACTED] |
| Surreal Enterprise | [REDACTED] |
| Secure Ryde LLC | [REDACTED] |
| Carbon Enterprise | [REDACTED] |
| Matchbox Denim LLC | [REDACTED] |
| Cake Talk Bakery | [REDACTED] |
| Brow Aesthetics LLC | [REDACTED] |
| End Staff Remolding a/k/a End Staff Remodeling | [REDACTED] |
| EDC Tooling | [REDACTED] |

- f. It was further part of the conspiracy that Defendants, unindicted co-conspirators, CW 1 and CW 2, and others known and unknown to the Grand Jury carried out the objectives of the conspiracy by using the following personal and business bank accounts, among others, at federally insured financial institutions:

| Bank | Account # | Controlled by |
|--------------------------------|-----------|---------------|
| Ascend Federal Credit Union | x8946 | [REDACTED] |

| Bank | Account # | Controlled by |
|----------------------------------|-----------|---|
| Ascend Federal Credit Union | x0920 | [REDACTED] held in the name of sham company Westwego Resources LLC |
| Ascend Federal Credit Union | x7865 | [REDACTED] held in the name of sham company R & MC Productions |
| Bank of America | x4341 | [REDACTED] held in the name of sham company Cake Talk Bakery |
| Bank of America | x3625 | [REDACTED] |
| Bank of America | x5873 | [REDACTED] held in the name of sham company Brow Aesthetics LLC |
| Bank of America | x4064 | [REDACTED] |
| Bank of America | x8356 | "Money mule" R.M |
| Bank of America | x6217 | "Money mules" D.V. and N.P., held in the name of D.V. and N.P.'s business |
| Diversified Members Credit Union | x3097 | "Money mule" J.B. |
| First Tennessee Bank | x0942 | [REDACTED], held in the name of sham company West Wego Resources |
| First Tennessee Bank | x0970 | [REDACTED] |
| First Tennessee Bank | x0928 | [REDACTED] |
| First Tennessee Bank | x0816 | [REDACTED] |
| First Tennessee Bank | x0420 | CW 1, held in the name of CW 1's business |

| Bank | Account # | Controlled by |
|---------------------------|-----------|--|
| First Tennessee Bank | x2645 | CW 1 |
| First Tennessee Bank | x3289 | [REDACTED] held in the name of sham company EDC Tooling |
| Fort Sill National Bank | x8127 | [REDACTED] |
| Fort Sill National Bank | x8290 | [REDACTED] and "money mule" D.T. |
| JPMorgan Chase | x2343 | [REDACTED] held in the name of sham company Matchbox Denim LLC |
| JPMorgan Chase | x5606 | [REDACTED] |
| JPMorgan Chase | x3655 | [REDACTED] held in the name of front company Secure Ryde LLC |
| Navy Federal Credit Union | x2951 | [REDACTED] |
| Navy Federal Credit Union | x2210 | [REDACTED] |
| Navy Federal Credit Union | x5664 | [REDACTED] |
| Regions Bank | x7495 | [REDACTED] held in the name of sham company End Staff Remodeling |
| Regions Bank | x0605 | [REDACTED] |
| Regions Bank | x5201 | [REDACTED] and "Money Mule" D.E., held in the name of sham company West Wego Resources |
| Regions Bank | x2631 | [REDACTED] |

| Bank | Account # | Controlled by |
|-----------------|-----------|--|
| Regions Bank | x3093 | "Money mule" D.W., held in the name of D.W.'s business |
| SunTrust | x1305 | "Money mule" Z.M., held in the name of Z.M.'s business |
| Wells Fargo | x4950 | CW 2, held in the name of CW 2's business |
| Wells Fargo | x2882 | "Money mule" S.H., held in the name of S.H.'s business |
| Woodforest Bank | x0279 | "Money mule" R.W., held in the name of R.W.'s business |

- g. It was further part of the conspiracy that Defendants, unindicted co-conspirators, and others known and unknown to the Grand Jury would quickly transfer, or cause to be transferred, fraudulent proceeds deposited into bank accounts identified above by making interstate and foreign wire transfers to other accounts controlled by Defendants and others known and unknown to the Grand Jury.
- h. It was further part of the conspiracy that Defendants, unindicted co-conspirators, and others known and unknown to the Grand Jury made, or caused to be made, cash and cashier's check withdrawals, and then deposited cash or cashier's checks into bank accounts controlled by Defendants, unindicted co-conspirators, and others known and unknown to the Grand Jury.
- i. It was further part of the conspiracy that Defendants, unindicted co-conspirators, and others known and unknown to the Grand Jury transferred, or caused to be transferred, fraudulent proceeds via peer-to-peer payment platforms and money service businesses to other Defendants, unindicted co-conspirators, and others known and unknown to the Grand Jury.

ACTS IN FURTHERANCE

37. In furtherance of the conspiracy and to bring about the object and goals of the conspiracy, including to conceal its nature and existence, Defendants [1] SAMSON A. OMONIYI, a/k/a "Dada," a/k/a "Dadaman81," a/k/a "Mr D"; [REDACTED]

[REDACTED] unindicted co-conspirators, and others known and unknown to the Grand Jury committed acts in the Middle District of Tennessee and elsewhere, including but not limited to, the following:

Money Laundering of COMPANY A Business Email Compromise Scheme Proceeds

- a. On or about November 28, 2016, [REDACTED] and D.E. conducted the following transactions from the Regions Bank account ending in x5201 with fraud proceeds derived from the BEC scheme against COMPANY A described in Paragraph 32(a):
 - i. \$40,000 wire transfer to a First Tennessee Bank account ending in x0942, controlled by [REDACTED], held in the name of sham company West Wego Resources; and
 - ii. \$47,000 wire transfer to a First Tennessee Bank account ending in x0970, controlled by [REDACTED]
- b. From on or about November 29, 2016, to on or about December 14, 2016, [REDACTED] conducted the following transactions, which represented fraud proceeds derived from the BEC scheme against COMPANY A described in

Paragraph 32(a), from [REDACTED] First Tennessee Bank account ending in x0942, held in the name of sham company West Wego Resources:

- i. \$3,000 transfer to a First Tennessee Bank account ending in x0928, controlled by [REDACTED]
 - ii. \$5,000 withdrawal; and
 - iii. \$18,000 withdrawal.
- c. On or about November 30, 2016, [REDACTED] transferred \$40,000, which represented fraud proceeds derived from the BEC scheme on COMPANY A described in Paragraph 32(a), from [REDACTED] First Tennessee Bank account ending in x0970 to a First Tennessee Bank account ending in x0816, controlled by [REDACTED]
- d. On or about November 30, 2016, [REDACTED] withdrew \$32,856.78 which represented fraud proceeds derived from the BEC scheme on COMPANY A described in Paragraph 32(a), from [REDACTED] First Tennessee Bank account ending in x0816.

Money Laundering of COMPANY B Business Email Compromise Scheme Proceeds

- e. Between on or about September 12, 2017, to on or about September 13, 2017, R.W. conducted the following transactions from the Woodforest Bank account ending in x0279 with fraud proceeds derived from the BEC scheme on COMPANY B described in Paragraph 32(b):
 - i. \$40,500 wire transfer to an Ascend Federal Credit Union account ending in x8946, controlled by [REDACTED]

- ii. \$40,500 wire transfer to an Ascend Federal Credit Union account ending in x0920, controlled by [REDACTED] held in the name of sham company Westwego Resources LLC; and
 - iii. \$27,000 wire transfer to an Ascend Federal Credit Union account ending in x0920, controlled by [REDACTED] held in the name of sham company Westwego Resources LLC.
- f. On or about September 14, 2017, “money mule” J.B. sent a \$47,215 wire transfer, which represented fraud proceeds derived from the BEC scheme on COMPANY B described in Paragraph 32(b), from the Diversified Members Credit Union bank account ending in x3097 to [REDACTED] Ascend Federal Credit Union bank account ending in x0920, held in the name of sham company Westwego Resources LLC.

Money Laundering of R.D. Business Email Compromise Scheme Proceeds

- g. On or about October 11, 2017, at approximately 11:22 a.m., [REDACTED] [REDACTED] withdrew \$9,500 in cash from the Ascend Federal Credit Union account ending in x7865, which represented fraud proceeds derived from the BEC scheme on COMPANY C described in Paragraph 32(c).
- h. On or about October 11, 2017, at approximately 4:22 p.m., [REDACTED] [REDACTED] using fraud proceeds derived from the BEC scheme on COMPANY C described in Paragraph 32(c), sent a Western Union payment to [1] SAMSON A. OMONIYI in the amount of \$400.

Money Laundering of COMPANY D Business Email Compromise Scheme Proceeds

- i. Between on or about June 8, 2018, to on or about June 9, 2018, [REDACTED] [REDACTED] conducted the following transactions from Regions Bank account ending in x7495 with fraud proceeds derived from the BEC scheme on COMPANY D described in Paragraph 32(d):

- i. \$23,000 cash withdrawal; and
- ii. \$18,000 cash withdrawal.

- j. Between on or about June 8, 2018, to on or about June 13, 2018, [REDACTED] [REDACTED] and [REDACTED] conducted the following transactions with fraud proceeds derived from the BEC scheme on COMPANY D described in Paragraph 32(d):

- i. [REDACTED] made a \$6,350 cash deposit into a Regions Bank account ending in x0605, controlled by [REDACTED] [REDACTED]
- ii. [REDACTED] made a \$5,000 cash deposit into a Regions Bank account ending in x0605, controlled by [REDACTED] [REDACTED] and [REDACTED]
- iii. [REDACTED] made a \$350 cash deposit into a Regions Bank account ending in x0605, controlled by [REDACTED] [REDACTED]

Money laundering of COMPANY E Business Email Compromise Scheme Proceeds

k. Between on or about July 17, 2018, to on or about July 20, 2018, at the direction of [REDACTED], CW 1 conducted the following transactions with fraud proceeds derived from the BEC on COMPANY E described in Paragraph 32(e):

- i. \$40,000 transfer to a First Tennessee Bank account ending in x2645, controlled by CW 1;
- ii. \$10,000 cash withdrawal;
- iii. \$5,000 cash withdrawal; and
- iv. \$1,860 Western Union payment transfer to [REDACTED]
[REDACTED]

l. On or about July 17, 2018, at the direction of [REDACTED] CW 1 withdrew \$36,000 in cash from the First Tennessee Bank account ending in x2645, controlled by CW 1, which represented fraud proceeds derived from the BEC on COMPANY E described in Paragraph 32(e).

Money Laundering of COMPANY F Business Email Compromise Scheme Proceeds

m. On or about September 13, 2018, [REDACTED] withdrew \$9,800 in cash at [REDACTED] direction from [REDACTED] First Tennessee Bank account ending in x3289 held in the name of sham company EDC Tooling, which represented fraud proceeds from the BEC scheme on COMPANY F described in Paragraph 32(f).

n. On or about September 13, 2018, at the direction of [REDACTED]
[REDACTED] conducted the following transactions with fraud proceeds derived from BEC scheme on COMPANY F described in Paragraph 32(f):

- i. \$5,000 cash deposit into a Regions Bank account ending in x0605, controlled by [REDACTED]; and
- ii. \$1,400 cash deposit into a Regions Bank account ending in x2631, controlled by [REDACTED], held in the name of sham company Carbon Enterprises.

Money Laundering of COMPANY G Business Email Compromise Scheme Proceeds

- o. Between on or about December 15, 2018, to on or about December 18, 2018, “money mule” Z.M. conducted the following transactions from the SunTrust Bank account ending in x1305 with fraud proceeds derived from the BEC scheme on COMPANY G described in Paragraph 32(g):
 - i. Obtained a \$5,000 cashier’s check made payable to [REDACTED]
[REDACTED]
 - ii. Obtained a \$20,000 cashier’s check made payable to [REDACTED]
[REDACTED]
 - iii. Obtained a \$20,000 cashier’s check made payable to [REDACTED]
[REDACTED]
 - iv. \$100,000 wire transfer to a Navy Federal Credit Union account ending in x2951, controlled by [REDACTED], held in the name of sham company Surreal Enterprises, which posted to the Surreal Enterprises bank account on or about December 17, 2018; and
 - v. \$5,487.91 transfer to US Bank for a home mortgage loan payment ending in x5364, in the name of [REDACTED]

p. Between on or about December 18, 2018, to on or about December 20, 2018, [REDACTED] conducted the following transactions from Surreal Enterprise's Navy Federal Credit Union account ending in x2951 with fraud proceeds derived from the BEC scheme on COMPANY G described in Paragraph 32(g):

- vi. Two \$5,000 wire transfers to a Fort Sill National Bank Account ending in x8127, controlled by [REDACTED]
- vii. \$10,000 wire transfer to a Navy Federal Credit Union account ending in x2210, controlled by [REDACTED]
- viii. \$10,472 cash withdrawal;
- ix. \$20,266 cash withdrawal; and
- x. \$15,000 cash withdrawal.

Money Laundering of COMPANY H Business Email Compromise Scheme Proceeds

q. Between on or about March 8, 2021, to on or about March 9, 2021, "money mule" D.V. conducted the following transactions from the Bank of America account ending in x6217 with fraud proceeds derived from the BEC scheme on COMPANY H described in Paragraph 32(h):

- i. Obtained a \$37,000 cashier's check made payable to [REDACTED] [REDACTED] sham company Matchbox Denim LLC, which posted to [REDACTED] JPMorgan Chase account ending in x2343, held in the name of her sham company Matchbox Denim LLC, on March 10, 2021; and

- ii. Obtained a \$21,500 cashier's check made payable to [REDACTED]
[REDACTED] sham company Matchbox Denim LLC, which posted to
[REDACTED] JPMorgan Chase account ending in
x2343, held in the name of her sham company Matchbox Denim LLC,
on March 10, 2021.
- r. Between on or about March 13, 2021, to on or about March 16, 2021,
[REDACTED] conducted the following transactions from the
JPMorgan Chase account ending in x2343, held in the name of her sham company
Matchbox Denim LLC, with fraud proceeds derived from the BEC scheme on
COMPANY H described in Paragraph 32(h):
 - iii. \$15,000 withdrawal;
 - iv. \$16,000 withdrawal; and
 - v. \$9,000 withdrawal.
- s. On or about May 20, 2021, D.V. obtained a \$15,200 cashier's check using fraud
proceeds derived from the BEC scheme on COMPANY H described in Paragraph
32(h), made payable to [REDACTED] sham company Matchbox
Denim LLC, which posted to [REDACTED] JPMorgan Chase
account ending in x2343 held in the name of her sham company Matchbox Denim
LLC, on or about May 24, 2021.
- t. On or about May 26, 2021, [REDACTED] sent a \$1,500 transfer, via
Zelle from [REDACTED] JPMorgan Chase account ending in
x2343 held in the name of her sham company Matchbox Denim LLC to

[1] **SAMSON A. OMONIYI** using fraud proceeds derived from the BEC scheme on COMPANY H described in Paragraph 32(h).

Money Laundering of COMPANY I Business Email Compromise Scheme Proceeds

- u. On or about April 21, 2021, “money mule” R.M. obtained a \$49,800 cashier’s check using fraud proceeds derived from the BEC scheme on COMPANY I described in Paragraph 32(i), from the Bank of America account ending in x8356, made payable to [REDACTED] sham company Matchbox Denim LLC, which posted to [REDACTED] JPMorgan Chase account ending in x2343, held in the name of her sham company Matchbox Denim LLC, the same day.
- v. Between on or about April 26, 2021, to on or about April 29, 2021, [REDACTED] conducted the following transactions from the JPMorgan Chase account ending in x2343 held in the name of sham company Matchbox Denim LLC with fraud proceeds derived from the BEC on COMPANY I described in Paragraph 32(i):
 - i. \$15,000 withdrawal; and
 - ii. \$9,500 withdrawal.
- w. On or about May 13, 2021, R.M. obtained a \$93,830 cashier’s check, using fraudulent proceeds derived from the BEC scheme on COMPANY I described in Paragraph 32(i), from the Bank of America account ending in x8356, made payable to [REDACTED] sham company Matchbox Denim LLC, which posted into [REDACTED] JPMorgan Chase account ending in x2343, held in the name of sham company Matchbox Denim LLC, the same day.

x. Between on or about May 14, 2021, to on or about May 21, 2021, [REDACTED] [REDACTED] conducted the following transactions from the JPMorgan Chase account ending in x2343 held in the name of her sham company Matchbox Denim LLC with fraud proceeds derived from the BEC scheme on COMPANY I described in Paragraph 32(i):

- i. \$2,500 transfer via Zelle to [1] SAMSON A. OMONIYI;
- ii. \$6,600 withdrawal;
- iii. \$8,000 withdrawal;
- iv. \$3,870 transfer via Zelle to [1] SAMSON A. OMONIYI; and
- v. \$60,000 withdrawal.

Money Laundering of COMPANY J Business Email Compromise Scheme Proceeds

y. Between on or about November 12, 2021, to on or about November 17, 2021, at the direction of [REDACTED] CW 2 conducted the following transactions with fraud proceeds derived from the BEC scheme on COMPANY J described in Paragraph 32(j):

- i. Three \$1,500 transfers via Cash App to [REDACTED] sham company Secure Ryde LLC;
- ii. \$20,000 wire transfer to a Navy Federal Credit Union account ending in x5664, controlled by [REDACTED]
- iii. Obtained a \$28,402 cashier's check made payable to Cake Talk Bakery, [REDACTED] sham company, which posted into a Bank of America account ending in x4341, controlled by

- [REDACTED] held in the name of sham company Cake Talk Bakery, on or about November 12, 2021;
- iv. Obtained a \$6,718 cashier's check made payable to Matchbox Denim LLC, [REDACTED] sham company, which posted to a JPMorgan Chase account ending in x2343, controlled by [REDACTED] held in the name of sham company Matchbox Denim LLC, on or about November 13, 2021; and
- v. Obtained a \$8,000 check made payable to [REDACTED]
- z. Between on or about November 15, 2021, to on or about November 29, 2021, [REDACTED] conducted the following transactions from the Bank of America account ending in x4341, held in the name of her sham company Cake Talk Bakery with fraud proceeds derived from the BEC scheme on COMPANY J described at Paragraph 32(j):
- i. Four transfers, totaling \$6,409, to a Bank of America account ending in x3625, controlled by [REDACTED]
- ii. Two \$3,000 transfers via Cash App to [1] SAMSON A. OMONIYI; and
- iii. \$3,500 transfer via Zelle to [REDACTED]
- aa. Between on or about November 24, 2021, to on or about November 29, 2021, [REDACTED] conducted the following transactions from the JPMorgan Chase account ending in x2343 held in the name of sham company Matchbox Denim LLC with fraud proceeds derived from the BEC scheme on COMPANY J described at Paragraph 32(j):

- i. \$1,500 transfer via Zelle to [1] **SAMSON A. OMONIYI**; and
- ii. \$3,500 transfer via Zelle to [1] **SAMSON A. OMONIYI**.

Money Laundering of R.P. Business Email Compromise Scheme Proceeds

bb. Between on or about March 29, 2022, to on or about March 30, 2022, “money mule” S.H. conducted the following transactions from the Wells Fargo account ending in x2882 with fraud proceeds derived from the BEC scheme on R.P. described in Paragraph 32(k):

- i. Obtained a \$31,000 cashier’s check made payable to Matchbox Denim LLC, [REDACTED] sham company, which posted to a JPMorgan Chase account ending in x2343, controlled by [REDACTED] held in the name of sham company Matchbox Denim LLC, on or about March 29, 2022;
- ii. Obtained a \$131,000 cashier’s check made payable to Matchbox Denim LLC, [REDACTED] sham company, which posted to [REDACTED] same JPMorgan Chase account ending in x2343, held in the name of sham company Matchbox Denim LLC, on or about March 31, 2022; and
- iii. Obtained a \$60,000 cashier’s check made payable to “money mule” P.S., which posted to [REDACTED] JPMorgan Chase account ending in x2343, held in the name of sham company Matchbox Denim LLC, on or about May 13, 2022.

cc. Between on or about March 31, 2022, to on or about April 18, 2022, [REDACTED] conducted the following transactions from the

JPMorgan Chase account ending in x2343 with fraud proceeds derived from the BEC scheme on R.P. described at Paragraph 32(k):

- i. \$24,220 withdrawal;
 - ii. \$20,000 withdrawal;
 - iii. \$500 transfer via Zelle to [1] **SAMSON A. OMONIYI**; and
 - iv. \$21,465 withdrawal.
- dd. Between on or about May 18, 2022, to on or about May 23, 2022, [REDACTED] sent five transfers via Zelle, totaling \$9,700, from the JPMorgan Chase account ending in x2343, held in the name of sham company Matchbox Denim LLC, to a JPMorgan Chase account ending in x5606, controlled by [REDACTED] using fraud proceeds derived from the BEC scheme on R.P. described in Paragraph 32(k).

Money Laundering of COMPANY L Business Email Compromise Scheme Proceeds

- ee. Between on or about June 24, 2022, to on or about July 11, 2022, “money mule” D.W. conducted the following transactions from the Regions Bank account ending in x3093 with fraud proceeds derived from the BEC scheme on COMPANY L described in Paragraph 32(l):
- i. Obtained a \$122,438 cashier’s check made payable to Brow Aesthetics LLC, [REDACTED] sham company, which posted to a Bank of America account ending in x5873, controlled by [REDACTED] [REDACTED] held in the name of sham company Brow Aesthetics LLC;
 - ii. Obtained a \$60,000 cashier’s check made payable to “money mule” D.T.;

- iii. Obtained a \$30,800 cashier's check made payable to Secure Ryde LLC, [REDACTED] front company, which posted to a JPMorgan Chase account ending in x3655, controlled by [REDACTED] held in the name of front company Secure Ryde LLC;
- iv. Three transfers, totaling \$3,700, via Cash App to [REDACTED] [REDACTED]
- v. Two transfers, totaling \$3,000, via Cash App to [REDACTED] and
- vi. \$1,500 transfer via Cash App to [REDACTED]
- ff. Between on or about June 27, 2022, to on or about July 7, 2022, [REDACTED] [REDACTED] sent six transfers via Zelle, totaling \$18,266, from the Bank of America account ending in x5873, held in the name of her sham company Brow Aesthetics LLC, to a Bank of America account ending in x4064, controlled by [REDACTED] [REDACTED] using fraud proceeds derived from the BEC scheme on COMPANY L described in Paragraph 32(l).
- gg. Between on or about July 6, 2022, to on or about July 7, 2022, [REDACTED] [REDACTED] conducted the following transactions from the Bank of America account ending in x4064 using fraud proceeds derived from the BEC scheme on COMPANY L described in Paragraph 32(l):
 - i. \$2,500 transfer via Cash App to [1] SAMSON A. OMONIYI; and
 - ii. \$5,000 transfer via Cash App to [1] SAMSON A. OMONIYI.
- hh. On or about June 27, 2022, "money mule" D.T. deposited the \$60,000 cashier's check, which was funded using fraud proceeds derived from the BEC scheme on

COMPANY L described in Paragraph 32(l), drawn from D.W.'s Regions Bank account ending in x3093, into a Fort Sill National Bank account ending in x8290, controlled by D.T. and [REDACTED]

- ii. Between on or about July 1, 2022, to on or about July 11, 2022, D.T. and [REDACTED] conducted the following transactions from the Fort Sill National Bank account ending in x8290 with fraud proceeds derived from the BEC on COMPANY L described in Paragraph 32(l):

- i. \$4,303 withdrawal;
- ii. Seven transfers, totaling \$675, via Cash App to [REDACTED]
[REDACTED] and [REDACTED];
- iii. Two transfers, totaling \$440, via Cash App to [REDACTED]

All in violation of Title 18, United States Code, Section 1956(h).

NOTICE OF FORFEITURE

Upon conviction of the offense alleged in Count One of this Indictment, the Defendants

[1] **SAMSON A. OMONIYI**, a/k/a "Dada," a/k/a "Dadaman81," a/k/a "Mr D," [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), as part of the sentencing pursuant to Federal Rule of Criminal Procedure 32.2, all property, real or personal, involved in such offense, and any property traceable to such property.

If the above-described forfeitable property, as a result of any act or omission of the defendant:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty;

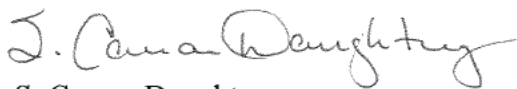
it is the intention of the United States of America to seek an order forfeiting substitute assets pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1) and Title 28, United States Code, Section 2461(c), and Federal Rule of Criminal Procedure 32.2(e).

A TRUE BILL



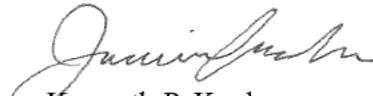
Foreperson

THOMAS J. JAWORSKI
Acting United States Attorney
Middle District of Tennessee



S. Carran Daughtrey
Assistant United States Attorney

MARGARET A. MOESER
Chief, Money Laundering & Asset Recovery Section
U.S. Department of Justice, Criminal Division



Kenneth P. Kaplan
Jasmin Salehi Fashami
Trial Attorneys

CRIMINAL COVER SHEET
MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

Indictment (x)
Complaint ()
Information ()
Felony (x)
Misdemeanor ()
Juvenile ()

County of Offense: Rutherford County
AUSA's NAME: S. Carran Daughtrey

Reviewed by AUSA: SCD
(Initials)

Samson A. OMONIYI
Defendant's Full Name

2209 Bastrop St, Houston, TX 77003
Defendant's Address

Interpreter Needed? _____ Yes x No

If Yes, what language? _____

Unknown
Defendant's Attorney

| COUNT(S) | TITLE/SECTION | OFFENSE CHARGED | MAX. PRISON (plus any mandatory minimum) | MAX. FINE |
|----------|---------------------|--|--|-----------|
| 1 | 18 U.S.C. § 1956(h) | Conspiracy to Launder Monetary Instruments | 20 years | \$500,000 |

Is the defendant currently in custody? Yes () No (x) If yes, State or Federal? Writ requested ()

Has a complaint been filed? Yes () No (x)

If Yes: Name of the Magistrate Judge _____ Case No.: _____
Was the defendant arrested on the complaint? Yes () No ()

Has a search warrant been issued? Yes (x) No () [see below]

If Yes: Name of the Magistrate Judge _____ Case No.: _____

Was bond set by Magistrate/District Judge? Yes () No () Amount of bond: _____

Is this a Rule 20? Yes () No (x) To/from what district? _____

Is this a Rule 40? Yes () No (x) To/from what district? _____

Estimated trial time: 3 to 4 weeks

The Clerk will issue a **Warrant** (Note: If information, request for a warrant requires presentment of a sworn affidavit of probable cause to a judicial officer, who will determine whether to issue a warrant)

Detention requested: Yes (x) No () Recommended conditions of release: _____

Search Warrants:

Judge Newbern: 19-MJ-4247; 19-MJ-4248; 19-MJ-4249; 19-MJ-4258; 20-MJ-4076; 24-MJ-4176; 24-MJ-4376
Judge Frensey: 19-MJ-2226
Judge Holmes: 21-MJ-1072; 21-MJ-1073; 21-MJ-1074